CLAIMS:

1. A method for reducing the boot time of a Trusted Computing Performance Alliance (TCPA) based computing system comprising the steps of:

resetting said TCPA computing system;

executing a boot block code comprising a Core Root of Trust Measurement (CRTM);

reading bits in a register of a flash memory storing said boot block code, wherein said bits in said register indicate whether segments of said flash memory have been updated; and

obtaining one or more measurement values from a table storing hashed values from a previous measurement of a Power On Self Test (POST) Basic Input/Output System (BIOS) if one or more of said bits read in said register indicate one or more of said segments of said flash memory storing said POST BIOS have not been updated.

2. The method as recited in claim 1 further comprising the step of:

transmitting said obtained measurement values to a Trusted Platform Module.

3. The method as recited in claim 2 further comprising the steps of:

setting a control bit in said register so no other device can set said bits read in said register; and

executing said POST BIOS.

4. The method as recited in claim 1 further comprising the steps of:

performing a measurement of a segment of said flash memory storing said POST BIOS which is indicated by a bit in said register as having been updated;

performing a look-up in said table of a previous measurement of said segment updated of said flash memory storing said POST BIOS; and

comparing said measured value with said looked-up value in said table.

5. The method as recited in claim 4 further comprising the step of:

taking appropriate security measures if said measured value is not equal with said looked-up value in said table.

6. The method as recited in claim 4 further comprising the step of:

resetting said bit in said register to indicate that said segment of said flash memory is validated if said measured value is equal with said looked-up value in said table.

7. The method as recited in 6 further comprising the step of:

transmitting said measured value of said segment of said flash memory updated and said obtained measurement values of one of more of said segments of said flash memory storing said POST BIOS that have not been updated to a Trusted Platform Module.

8. A computer program product embodied in a machine readable medium for reducing the boot time of a Trusted Computing Performance Alliance (TCPA) based computing system comprising the programming steps of:

executing a boot block code comprising a Core Root of Trust Measurement (CRTM);

reading bits in a register of a flash memory storing said boot block code, wherein said bits in said register indicate whether segments of said flash memory have been updated; and

obtaining one or more measurement values from a table storing hashed values from a previous measurement of a Power On Self Test (POST) Basic Input/Output System (BIOS) if one or more of said bits read in said register indicate one or more of said segments of said flash memory storing said POST BIOS have not been updated.

9. The computer program product as recited in claim 8 further comprising the programming step of:

transmitting said obtained measurement values to a Trusted Platform Module.

10. The computer program product as recited in claim 9 further comprising the programming steps of:

setting a control bit in said register so no other device can set said bits read in said register; and

executing said POST BIOS.

11. The computer program product as recited in claim 8 further comprising the programming steps of:

performing a measurement of a segment of said flash memory storing said POST BIOS which is indicated by a bit in said register as having been updated;

performing a look-up in said table of a previous measurement of said segment updated of said flash memory storing said POST BIOS; and

comparing said measured value with said looked-up value in said table.

12. The computer program product as recited in claim 11 further comprising the programming step of:

taking appropriate security measures if said measured value is not equal with said looked-up value in said table.

13. The computer program product as recited in claim 11 further comprising the programming step of:

resetting said bit in said register to indicate that said segment of said flash memory is validated if said measured value is equal with said looked-up value in said table.

14. The computer program product as recited in 13 further comprising the programming step of:

transmitting said measured value of said segment of said flash memory updated and said obtained measurement values of one of more of said segments of said flash memory storing said POST BIOS that have not been updated to a Trusted Platform Module.

15. A system, comprising:

a processor;

a Trusted Building Block (TBB) coupled to said processor, wherein said TBB is configured to ensure integrity of said system, wherein said TBB comprises:

a Trusted Platform Module (TPM) configured to implement cryptographic algorithms; and

a portion of a flash memory coupled to said TPM, wherein said flash memory in said TBB comprises:

a register comprising bits configured to indicate whether segments of said flash memory have been updated;

a table configured to store measurements of a Power On Self Test (POST) Basic Input/Output System (BIOS) code stored in one or more segments of said flash memory; and

a boot block code, wherein said boot block code comprises code to reset said system, wherein said boot block code comprises a Core Root of Trust for Measurement (CRTM) configured to measure said POST BIOS code;

wherein said processor, responsive to said CRTM, comprises:

circuitry operable for executing said boot block code;

circuitry operable for reading said bits in said register of said flash memory; and

circuitry operable for obtaining one or more measurement values from said table if one or more of said bits read in said register indicate one or more of said segments of said flash memory storing said POST BIOS code have not been updated.

16. The system as recited in claim 15, wherein said processor further comprises:

circuitry operable for transmitting said obtained measurement values to said TPM.

17. The system as recited in claim 16, wherein said processor further comprises:

circuitry operable for setting a control bit in said register so no other device can set said bits read in said register; and

circuitry operable for executing said POST BIOS code.

18. The system as recited in claim 15, wherein said processor further comprises:

circuitry operable for performing a measurement of a segment of said flash memory storing said POST BIOS code which is indicated by a bit in said register as having been updated;

circuitry operable for performing a look-up in said table of a previous measurement of said segment of said flash memory storing said POST BIOS code; and

circuitry operable for comparing said measured value with said looked-up value in said table.

19. The system as recited in claim 18, wherein said processor further comprises:

circuitry operable for taking appropriate security measures if said measured value is not equal with said looked-up value in said table.

20. The system as recited in claim 18, wherein said processor further comprises:

circuitry operable for resetting said bit in said register to indicate that said segment of said flash memory is validated if said measured value is equal with said looked-up value in said table.

21. The system as recited in claim 20, wherein said processor further comprises:

circuitry operable for transmitting said measured value of said segment of said flash memory updated and said obtained measurement values of one or more of said segments of said flash memory storing said POST BIOS code that have not been updated to said TPM.